BLAD GEMEENSCHAPPELIJKE REGELING
Nr. 363
11 november 2015

Officiële uitgave van gemeenschappelijke regeling WerkSaam Westfriesland.

INFORMATIEBEVEILIGINGSBELEID SUWINET

Gemeente Hoorn
WerkSaam

1. Inleiding

Dit informatiebeveiligingsbeleid Suwinet is een aanvulling op het organisatie brede informatiebeveiligingsbeleid. Iedere gemeente moet in een beveiligingsplan aangeven op welke wijze invulling is gegeven aan de beveiliging van de gegevensuitwisseling in het kader van Suwinet.

De organisaties die Suwinet gebruiken zijn verplicht zich te houden aan de eisen voor privacy en beveiliging. De Wet Bescherming Persoonsgegevens en de Suwi-wetgeving is hierop van toepassing. Het normenkader is te vinden in bijlage 1 Normenkader.

2. Rolverdeling en bijbehorende verantwoordelijkheden

Hieronder is beschreven wie welke rol heeft in de informatiebeveiliging:
1. Uitvoering van taken --> gebruikers Suwinet-Inkijk
2. Het beheer van autorisaties --> applicatiebeheerder Suwinet
3. Kwaliteitszorg en borging van rechtmatig gebruik --> beveiligingscoördinator
4. Optreden bij oneigenlijk gebruik of misbruik Suwinet --> management en de beveiligingscoördinator
5. Uitdragen goed gebruik--> management en de beveiligingscoördinator.

In bijlage 2 Gebruikers Suwinet is beschreven welke rollen voor welke taken autorisatie kunnen krijgen.

2.1 Taakomschrijving beveiligingscoördinator

De beveiligingscoördinator:
1. is verantwoordelijk voor het beheer, onderhoud en evaluatie van het informatiebeveiligingsbeleid Suwinet
2. informeert, bevordert en adviseert over de informatiebeveiliging van Suwinet
3. controleert of het informatiebeveiligingsbeleid Suwinet en de procedures worden nageleefd controleert de Suwinet autorisaties
4. controleert de rapportages van Suwinet.
5. rapporteert bevindingen rechtstreeks aan het hoogste management.

3. Informatiebeveiliging Suwinet medewerkers

Voor het werken en omgaan met persoonsgebonden gegevens binnen de overheid zijn in de Wet bescherming persoonsgegeven (Wbp) regels opgesteld. Binnen de wet Suwi zijn geheimhoudingsbepalingen opgenomen waarin is bepaald dat de persoonsgegevens niet verder bekend gemaakt mogen worden dan voor de uitoefening van de functie noodzakelijk is. Daarnaast is artikel 125a van de ambtenarenwet geheimhouding opgelegd aan ambtenaren. Vaste, tijdelijke en externe medewerkers van de gemeente Hoorn en WerkSaam met een autorisatie voor Suwinet-Inkijk moeten een zorgvuldigheidsverklaring (zie bijlage 3) ondertekenen.

De wijze waarop de autorisaties worden toegekend, gewijzigd of ingetrokken is nader geregeld in de Autorisatieprocedure Suwinet (zie bijlage 4).

4. Bewustwording medewerkers

Om de bewustwording te vergroten onder de medewerkers worden de volgende acties uitgevoerd:

1. Het beveiligingsplan Suwinet is gepubliceerd op intranet.
2. Gebruikers van Suwinet-Inkijk moeten weten dat over hen gegevens worden vastgelegd en verzameld. Dit is een belangrijk onderdeel van de privacybescherming ten opzichte van onze medewerkers. Aan de gebruikers van Suwinet-Inkijk is de volgende informatie verstrekt:

   - Informatiebeveiligingsbeleid Suwinet-Inkijk;
   - Het bestaan van de logging-applicatie;
   - De (aard van de) gegevens die worden verzameld;
   - Doelen van logging;
   - Het gebruik van de gelogde gegevens;
   - De gevolgen van misbruik.

3. Tijdens de algemene introductie van nieuwe medewerkers worden medewerkers geïnformeerd over het gebruik van privacygevoelige informatie.
4. Periodiek worden ten aanzien van informatiebeveiliging voor de bewustwording van de medewerkers artikelen op intranet geplaatst.

5. Evaluatie Informatiebeveiligingsplan Suwinet

Het informatiebeveiligingsbeleid wordt jaarlijks geëvalueerd en indien nodig geactualiseerd. De geconstateerde afwijkingen worden vastgelegd in de evaluatie en er wordt een voorstel ter voorkoming van de afwijkingen gedaan. De beveiligingscoördinator biedt de evaluatie ter vaststelling aan het hoogste management aan.

5.1 Rapportage gebruik Suwinet-Inkijk

Het Bureau Keteninformatiesering Werk en Inkomen (BKWI) stelt geanonimiseerde rapporten op met log gegevens van het gebruik van Suwinet-Inkijk (welke gegevens zijn hoe vaak geraadpleegd). Aan de hand van deze rapporten controleert de beveiligingscoördinator periodiek of er onjuist gebruik of misbruik is gemaakt van Suwinet-Inkijk. Als het vermoeden van ongeoorloofd gebruik van dat medium bestaat kan specifieke informatie per onderdeel of per medewerker bij het BKWI worden opgevraagd.

5.2 (Vermoeden van) beveiligingsincidenten

(Vermoedens van) beveiligingsincidenten worden gemeld bij de beveiligingscoördinator, waarna er een onderzoek wordt ingesteld. Indien uit onderzoek blijkt dat incidenten gegrond zijn, worden deze direct gerapporteerd aan de directie. Overige vermoedens en onderzoeken worden meegenomen in de jaarlijkse evaluatie.

Bijlage 1. Normenkader

De onderstaande regelgeving is van toepassing

1. Grondwet
2. Ambtenarenwet
3. Wet Bescherming Persoonsgegevens (Wpb)
4. Wet Eenmalige Gegevensuitvraag Werk en Inkomen (WEU)
5. Wet structuur uitvoeringsorganisatie werk en inkomen (Wet Suwi)
6. Besluit Suwi
7. Regeling Suwi
8. Besluit experimenten Suwi
9. Gedragskaart van de gemeente Hoorn

Bijlage 2. Gebruikers Suwinet

In onderstaande overzicht wordt per functie aangegeven in welke gevallen Suwinet-Inkijk gebruikt mag worden. We spreken in die gevallen van geoorloofd gebruik. Wordt Suwinet om andere redenen gebruikt dan hieronder verwoord, dan is er in principe sprake van ongeoorloofd gebruik. Raadplegen van Suwinet-Inkijk in andere situaties wordt gemotiveerd in de rapportage.

Er is een zodanig onderscheid gemaakt in functie en rol binnen de autorisatiestructuur van Suwinet dat de medewerker de voor hem/haar van belang zijnde gegevens kan raadplegen.

Afspraken over gebruik Suwine-inkijk:

Consulent Werk en Inkomen
Raadplegen als het de Wwb, Ioaw, Ioaz, Bbz of een andere door de afdeling uitgevoerde regeling betreft bij:

1. het behandelen van aanvragen of melding dat belanghebbende een uitkering wil aanvragen
2. in gevallen ter beoordeling van de medewerker. De reden van raadplegen van Suwinet-Inkijk wordt in die gevallen gemotiveerd in de rapportage van de medewerker.
3. rechtmatigheidsonderzoeken en tussenonderzoeken.

Medewerker terugvordering & verhaal WerkSaam
Raadplegen als het de Wwb, Ioaw, Ioaz, Bbz of een andere door de afdeling uitgevoerde regeling betreft bij onderzoeken die samenhangen met verhaal op onderhoudsplichtigen of vorderingen. Dit bijvoorbeeld ter vaststelling van woonplaats, draagkracht, inkomen of werkgever.

Kwaliteitsbeoordelaar (KBO) WerkSaam/gemeente
Raadplegen om besluiten te kunnen toetsen op het gebied van de WWB.

Medewerkers sociale recherche WerkSaam
Raadplegen in geval van fraude onderzoeken.

Medewerker burgerzaken gemeente
Raadplegen om adresonderzoeken te behandelen.

Medewerker RMC gemeente
Raadplegen om te onderzoeken of jongeren wel of geen werk hebben.

Medewerker invordering gemeentelijke belastingdeurwaarders
Ophalen van gegevens in geval van een dwangbevel.

Applicatiebeheerder WerkSaam/Gemeente
Voor het verzorgen van autorisaties voor Suwinet.

Zorgvuldigheidsverklaring

Ondergetekende:
Naam: ……………………………………………………………………………………………………
Organisatie: ……………………………………………………………………………………………………
Functie: ……………………………………………………………………………………………………
Datum:
……………………………………………………………………………………………………

BELOOFT/VERKLAART:

1. op de hoogte te zijn van de privacy en Suwi wet- en regelgeving
2. zich te houden aan de privacy en Suwi wet- en regelgeving
3. zorgvuldig om te gaan met de (persoons)gegevens en de inhoud van de documenten die bij de uitvoering van de werkzaamheden in Suwi-verband zijn ingezien.
4. zich te houden aan de werkinstructies zoals opgenomen in de functionele beschrijvingen van Suwinet-Inkijk. Dit betekent onder meer dat:

   - niet meer of vaker (persoons)gegevens worden geraadpleegd dan strikt noodzakelijk is;
   - een eigen registratie wordt bijgehouden van personen die niet voorkomen in een werkproces of module fraude en doel van opvraging;
   - (persoons)gegevens niet aan onbevoegden worden verstrekt;

5. het Suwinet-account en wachtwoord zorgvuldig en strikt persoonlijk te gebruiken en niet aan anderen ter beschikking te stellen.
6. op de hoogte te zijn van de inhoud van het algemene informatiebeveiligingsbeleid van de organisatie en het beveiligingsplan Suwinet.
7. gedurende de duur van de werkzaamheden in Suwinet-verband en ook na beëindiging van deze werkzaamheden, geheimhouding te betrachten met betrekking tot alle (persoons)gegevens.

8. bekend te zijn dat in het kader van interne controle alle BSN-nummers die zijn geraadpleegd via Suwinet-Inkijk opgevraagd worden.
9. bekend te zijn dat bij het vermoeden van onrechtmatig gebruik of misbruik van Suwinet-gegevens een onderzoek wordt gestart. Bij vaststelling van onrechtmatig handelen of van misbruik worden passende maatregelen getroffen.

Handtekening medewerker:

Bijlage 4. Autorisatieprocedure Suwinet

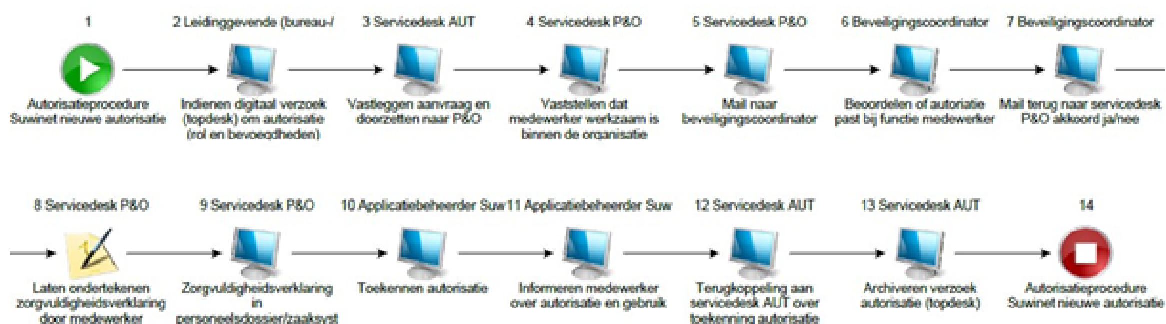
Deze procedure maakt deel uit van het Informatiebeveiligingsbeleid Suwinet. Deze procedure voorziet in het vastleggen van de verschillende stappen die noodzakelijk zijn voor het autoriseren van personen voor de toegang tot Suwinet. Hiermee wordt de logische toegangsbeveiliging afgedicht voor de daarin opgenomen gegevens en de vertrouwelijkheid gewaarborgd indien het raadplegen door medewerkers plaatsvindt.

De procedure bestaat uit afzonderlijke deelprocedures die gescheiden kunnen worden uitgevoerd:

1. Autorisatie tot de Suwinet. (Suwinet-Inkijk)
2. Functiewijziging of einde dienstverband/opdracht
3. Controle op autorisaties

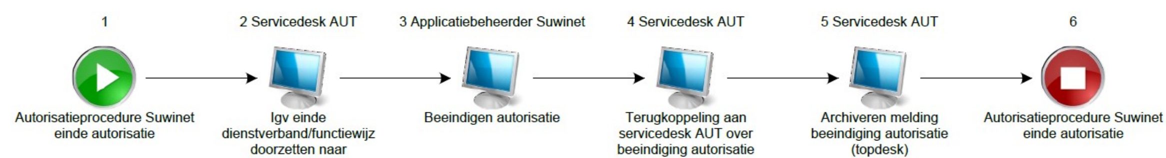
Uitgangspunten:
1. Toegang is verleend op basis van de uit te voeren functie / taken
2. Het uniek identificeren van elke gebruiker tot één persoon
3. De aanvraag voor toegangsrechten is gedaan door de manager of een gemandateerde
4. Bij functiewijziging of vertrek is de autorisatie direct aangepast
5. Suwinet-account en wachtwoord zijn herleidbaar naar één persoon en worden niet aan anderen/meerdere ter beschikking gesteld.
6. Het afdelingshoofd is eindverantwoordelijk voor het gebruik en de beveiliging van Suwinet Inkijk.
7. Applicatiebeheerders hebben een Suwinet beheeraccount. Zij hebben geen toegang tot persoonsgegevens.

Autorisatieprocedure:
1. De leidinggevende dient digitaal een autorisatieverzoek in voor een medewerker (vast, tijdelijk of inhuur) voor een autorisatie in Suwinet\. De taakinhoud/functie van de medewerker is hierin verwoord. De servicedesk registreert de melding en zet het door naar de servicedesk P&O.
2. Het autorisatieverzoek wordt beoordeeld door de servicedesk P&O. Er wordt vastgesteld of de verzoeker in het personeelsbestand voorkomt.
3. De servicedesk P&O zet de aanvraag door naar de beveiligingscoördinator die beoordeelt of de autorisatie past bij de functie van de medewerker.
4. Na goedkeuring van de beveiligingscoördinator zorgt de servicedesk P&O voor ondertekening van de zorgvuldigheidsverklaring door de medewerker. Een afschrift van deze verklaring wordt vastgelegd in het personeelsdossier of het zaaksysteem (inkoopzaak externe).
5. De applicatiebeheerder Suwinet ontvangt het autorisatieverzoek via de servicedesk P&O en kent de autorisatie toe. Een medewerker ontvangt alleen de autorisatie die volgens de autorisatiematrix passend is bij de functie van de medewerker.
6. De applicatiebeheerder informeert de medewerker over het gebruik van Suwinet en over de onderwerpen genoemd onder hoofdstuk 4 van het informatiebeveiligingsbeleid Suwinet.
7. De applicatiebeheerder koppelt terug naar de servicedesk AUT dat het autorisatieverzoek is toegekend.
8. De servicedesk AUT/applicatiebeheer archiveert het autorisatieverzoek.



Functiewijziging of einde dienstverband/opdracht

1. De leidinggevende is verantwoordelijk voor het doorgeven van een functiewijziging of einde dienstverband/opdracht aan de servicedesk. Een melding van einde dienstverband/opdracht of functiewijzing kan ook via een andere weg bij de servicedesk terecht komen.
2. Indien is geregistreerd dat de medewerker autorisatie heeft tot Suwinet, zet de servicedesk AUT de melding (ook) door naar de applicatiebeheerder Suwinet.
3. De applicatiebeheerder Suwinet beëindigt de autorisatie per de opgegeven einddatum.
4. De applicatiebeheerder Suwinet informeert de servicedesk over de beëindiging van de autorisatie.
5. De servicedesk archiveert de melding tot beëindigen autorisatie.



Controle op autorisaties

1. Minimaal 1x per jaar controleert de beveiligingscoördinator zichtbaar of:

   - Degene die toegang hebben tot Suwinet werkzaam zijn (vast, tijdelijk of extern) binnen de organisatie.
   - Degene die toegang hebben tot Suwinet een rol hebben die past bij de functie.
   - Suwinet gebruikt wordt:

   a. door gebruikers die 4 weken niet zijn ingelogd, wordt de autorisatie in overleg met de leidinggevende en applicatiebeheer beëindigd.
   b. door gebruikers die gedurende een lange periode niet zijn ingelogd, terwijl dit wel verwacht mag worden gezien de functie van de gebruiker, wordt nagegaan waarom niet is ingelogd. Dit kan duiden op gebruik van een ander zijn autorisatie.

2. De beveiliging coördinator rapporteert bevindingen aan de leidinggevende. Daarnaast worden bevindingen opgenomen in de jaarlijkse evaluatie aan het hoogste management, tenzij de bevindingen zo ernstig zijn dat er direct gerapporteerd moet worden.
3. De controle, bevindingen en rapportage wordt digitaal gearchiveerd.